Building Beyond the Foundation:
Accelerating the Delivery of the Information Sharing Environment
As Prepared for Delivery by Kshemendra Paul, PM-ISE
October 5, 2010

Acknowledgments

Good Morning. Thank you, Ozzie, for your kind introduction. I am grateful to CSIS for hosting today's conference. This is a wonderful forum in which to explore the challenges and opportunities around accelerating delivery of the Information Sharing Environment. Including clarifying its scope, mission and purpose; the target vision towards which we are building; and how we measure the created value.

We have the high calling, to support our mission partners – the federal, state and local agencies, private sector & foreign partners and members of the private sector in their counter-terrorism mission to protect the American people and enhance our National Security through the effective use of information.

Thank you to our sponsors today. We're grateful that you are supporting CSIS in continuing to shine a light on information sharing. There is a great line up of speakers and moderators, and I appreciate them taking the time to participate in the dialog today.

ISE – Background and the Building the Foundation

My communications team asked me to shamelessly promote the ISE community's web site – www.ise.gov – as a resource for folks who want to dig deeper and learn more about our collective efforts. While you're at the site – www.ise.gov – please be sure to sign up for e-mail alerts . . .

Before I get in to the meat of my remarks today, let me walk you through the structure of my presentation this morning. As Ozzie described, I am an engineer by training and was an Enterprise Architect while at Justice and the Office of Management and Budget. At times like this I feel the need to stay current in my functional domain. So please indulge me as I use a little EA parlance to describe my remarks this morning:

- First, I'll spend a little time looking back at how we got to we are today. This is the "as is".
- Next, I'll walk you through what we are hearing from thought leaders about where the ISE needs to go in the future. This is the "to be" – which will be shaped by our forum today.
- Then, I'll outline for you some of the really hard questions I need help answering. This is what GAO asked us when they came knocking . . . just kidding, just a big hello to my colleagues from the GAO . . .
- In our remaining time, I hope we'll move to questions & answers.

You don't often find engineers behind podiums addressing large crowds. You find us in dark, dank offices at odd hours, noodling and debating hard, technical problems. Or out in the field working to understand customer requirements and deliver solutions.

As an engineer, my approach to solving hard problems is rooted in an appreciation for first principles, diving headfirst into the details of the problem, and then lifting up and working the solution. This is the approach I am bringing to accelerating the delivery of the ISE.

One more sidebar – the ISE is an abstract topic and it's useful to set a mental model to help process the rest of what you hear today. Four examples of the ISE in action today:

- A Law Enforcement Officer – as part of a routine traffic stop, queries the National Crime Information Center and is notified to contact the Terrorist Screening Center to evaluate a potential match against the Terrorist Watchlist.
- An Intelligence Analyst using the National Library of Intelligence or A-Space platform to collaboratively develop new counter-terrorism intelligence products.
- Coast Guard personnel working on the Gulf Oil Spill and using DHS' Homeland Security Information Network and FEMA's Web Emergency Operating Center (the same assets to be leveraged to respond to both man-made and natural disasters)
- Finally, a local Law Enforcement Analyst and an FBI Analyst, co-located at the State Fusion Center, working prison radicalization – both developing finished intelligence products as well as supporting specific Joint Terrorism Task Force investigations

Back to the main part of my remarks – first up is to outline how we got here. As an engineer, I make a concerted effort to stay away from authorities discussions. But after 5 years in Washington – and three months as PM – I've learned to start with the authorities and mandate.

Origin, Authorities and Mission

In 2004, the 9-11 Commission delivered their report. The commission prescribed the need to transform and brought to light multiple challenges to 'connecting the dots.'

As an aside, I'm not a big fan of that term, because it oversimplifies the challenges – it does not provide a good frame for working through legitimate policy concerns, and does not help with the so-called "information overload problem".

The 9/11 Commission proposed that information "be shared horizontally, across (new) networks that transcend individual agencies"[1]. The Commission called for a "decentralized network model," that would allow agencies to maintain their own databases, but enable the databases to be "searchable across agency lines." It recognized, that by moving to a data-centric model a new framework would have to be established to control access to the data, and not the individual networks.

The Commission called for a government-wide effort to address the legal, policy, and technical issues that would arise from this type of system. The idea was to have someone looking across

[1] Ibid. Pg 418

agencies, creating a "Trusted Information Network" to facilitate the sharing of terrorism-related information.

This recommendation, amongst several others, was adopted from the 2003 Markle Report, "Creating a Trusted Information Network for Homeland Security". I know because I re-read it at the beach this summer!

This concept, as well as federated identity management, decentralized information, privacy protection, extensibility to state, local and tribal governments and a focus on prevention were incorporated into the Intelligence Reform and Terrorism Prevention Act of 2004 or IRTPA. They called it the Information Sharing Environment.

The Congress agreed with the 9/11 Commission that "Horizontal Integration" requires "government-wide" authority. So they created the role of a Program Manager to plan for, oversee and manage the Information Sharing Environment and granted the role government-wide authority.

The PM-ISE was told to work across 5 Communities: Intelligence, Defense, Law Enforcement, Homeland Security, and Foreign Affairs – and ensure the Environment enabled effective sharing of terrorism-related information.

The recognition that this effort had to have Horizontal Capabilities lay as much in the implications of technology issues as it did in the legal, policy, cultural, and organizational hurdles which needed to be overcome in order for process to succeed.

Subsequently, the "Implementing the Recommendations of the 9/11 Commission Act of 2007" amended IRTPA to expand the scope of the ISE to include homeland security and WMD information. The 9/11 Act also enhanced the authorities of the PM-ISE in two ways:

- First, it enhanced ability to issue government-wide procedures, guidelines, instructions, and functional standards; and
- Second, it mandated that we identify and resolve, with mission partners, information sharing disputes.

Foundational Steps

OK, I am done channeling my inner policy wonk. Now for the second part of the "as is" - what's been done to date? A strong foundation has been built and I'm going to describe a number of steps we've taken together as a Government.

In 2005, the Presidential Guidelines directed that the ISE leverage existing systems to the maximum extent practicable and directed that common information sharing standards be developed.

I need to pause here and emphasize the implications of these requirements. It is essential to understand that the ISE is owned and operated by mission partners – Federal, State, local, Tribal, and Territorial agencies, and our private sector and international partners. We as the PM-ISE don't build anything. We are not operational.

Our role is to help agencies find common mission equities, to help them implement functional and technical standards, and to drive resolution of policy issues. The actual point of implementation, the heavy lift, is with the agencies. They are the engines that deliver the ISE. They are the stars of the ISE.

The Guidelines also directed us to address the proliferation of Sensitive But Unclassified markings, develop a framework for privacy and civil liberties protections, and develop a common approach to sharing with State, local and tribal partners.

Much of the result of this work was captured in the 2007 National Strategy for Information Sharing and in subsequent ISE Annual Reports. These reports can be found at the ISE community web site. I want to highlight four areas:

- First up: Privacy and Civil Liberties. The ISE is envisioned as a trusted partnership of agencies at all levels of government and the private sector. In order to participate in the ISE, the law requires Federal departments and agencies – and our non-Federal partners – implement protections "at least as comprehensive as" the ISE Privacy Guidelines.

- Next, CUI – or Controlled Unclassified Information. The new CUI Framework will standardize more than 100 unique markings currently used for Sensitive But Unclassified information. These are the markings you see on the top of documents around town --- FOUO, OUO, LES and others. This standardization will be a critical step towards removing barriers to information sharing.
- Next, we developed the ISE Architecture-driven methodology to connect distributed and diverse ISE participant systems.
- Finally, Common Information Sharing Standards that document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting information sharing. The program was successfully used to standardize Suspicious Activity Reporting.

There are many other critical foundational "building blocks" for the ISE. Some examples are: Performance Measures, Identity and Access Management, Information Assurance, Culture, Training, and others. You can find the rest of the story at the ISE community web site.

<u>Emphasis on Information Sharing between Federal and State, Local, Tribal, and Territorial Governments</u>

Beyond the ISE's foundational enablers – much work has been done to help build up ISE Core Capabilities in the area of sharing with State, local, Tribal, and Territorial governments.

To develop the "common framework" we worked closely with stakeholders. In particular, I'd like to acknowledge our State, local, Tribal, Territorial and private sector partners. We worked with many organizations and individuals, I am going to miss someone, but I did want to try to highlight our partners. We worked with the:

- Criminal Intelligence Coordinating Council – known as the CICC,
- the Global Justice Information Sharing Initiative,
- the National Governor's Association's Governor's Homeland Security Advisors Council,
- the International Association of Chiefs of Police,
- Major Cities Chiefs Association,
- National Sheriff's Association,
- National Association of State CIOs,
- National Association of Counties,
- Owners and operators of critical infrastructure, and
- Many, many others.

The result was a series of recommendations to enhance the sharing of terrorism information across all levels of governments and the private sector.

One highlight of the work is the establishment of a national, integrated network of state and major urban area fusion centers. DHS is the executive agent with the lead for this part of the framework. Fusion centers are critical nodes that connect State, local, Tribal, and Territorial governments to the ISE. Through these fusion centers, state and major urban areas will be able to:

- Receive classified and unclassified federal information, including urgent, time sensitive alerts and warnings;
- Conduct risk assessments – potential threats, vulnerabilities, and consequences – based on their specific areas of operation;
- Further disseminate critical information to state, local, tribal and territorial authorities, and private sector entities within their jurisdiction, in coordination with Federal officials; and
- Gather, interpret, and disseminate local and state level information to other localities, states and to the Federal Government.

They will operate these capabilities within the scope of privacy policies – currently 26 Fusion Centers have privacy policies – up from 22 last month. These policies are "at least as comprehensive" as our privacy guidelines. With DHS's leadership we have solid momentum across the States to get the rest done in the coming year.

The framework just described is laid out in the 2007 National Strategy for Information Sharing. The Appendix of the Strategy defines, in great and useful detail, the Roles and Responsibilities for all levels of governments. And it is in the process of being implemented.

Bart Johnson, DHS Principal Deputy Under Secretary for Intelligence and Analysis is leading these efforts on behalf of DHS Secretary Napolitano and Under Secretary Wagner. Bart has an

incredible perspective on these matters, having spent most of his career with the New York State Police, culminating in commanding the Upstate New York State Regional Fusion Center. And just as he was getting it humming, the Feds hired him away. Bart is a friend; he is participating in the panel immediately following my talk.

Agency or Community-Based Improvements

We have also seen significant information sharing improvements within individual agencies. I'd like to highlight two examples from the Intelligence Community, that incidentally, my Office has had little direct involvement in accomplishing. That's the nice thing about being government-wide . . . Seriously; a core part of my responsibility is identifying, integrating, and extending best practices across the ISE.

Perhaps the most significant and visible change in terrorism-related "information sharing" was the establishment of the National Counterterrorism Center (NCTC). Russ Travers also is going to speak on the opening panel. He's NCTC's equivalent of a chief knowledge officer.
Russ is a respected leader in our community – he was recognized as a Galileo Award finalist this year for his thought leadership on information sharing.

Further, the Intelligence Community has led information integration by implementing IC Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information." This policy promotes responsible information sharing by distinguishing between discovery (obtaining knowledge that information exists) and dissemination or retrieval (obtaining the contents of the information).

There are many more improvements we documented in our Annual Report and highlighted on the ISE community web site.

Nationwide SAR Initiative – the ISE in Action

Before we turn our attention to the future…there is one last element of the ISE story to round out the "as is". And it's important to highlight because it helps make the meaning and value of the ISE that much more real.

In response to the 2007 National Strategy, we convened several federal agencies, law enforcement associations, local police departments, and others to develop a unified process for Suspicious Activity Reporting - or SAR.

This unified process builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a standardized process whereby that information can be shared among agencies to help detect and prevent terrorism-related criminal activity.

Tom O'Reilly, who presented here at CSIS a few weeks back, spoke at length about what is now called the Nationwide Suspicious Activity Reporting Initiative or NSI. Tom is a friend and someone I am privileged to call a mentor.

In March of this year, the Attorney General announced the establishment of a Program Office to facilitate the implementation of the NSI across all levels of government, and named Tom O'Reilly the Director. Tom's charge is to rollout the NSI nationwide, while ensuring that privacy, civil rights, and civil liberties are protected.

The NSI is one of our most significant accomplishments to-date and an example of the ISE in action:

> An interrelated set of harmonized policies, mission processes, and systems which leverage ISE core capabilities and enablers to empower the men and women on the frontline to access and share the information they need to keep the country safe.

And I have late breaking news. Now, the FBI is already integrated into the NSI solution. Last week, the FBI extended their integration to improve sharing of SARs generated from their field work. What is noteworthy here, and slightly technical, is that these SARs, while unclassified, are coming from their classified workflow systems and databases. It's a great example of being data-centric in our sharing, and sharing Federal data with other levels of Government.

Moving Forward

Which brings us to the "to be" part of my presentation today and the purpose of this forum. My Office is leading the process, with mission partners, of developing the National ISE Strategy. This includes subsuming the 2007 National Strategy for Information Sharing and bringing forward the foundational pieces of that document as it relates to our work with State, local, and Tribal stakeholders.

We are working with our mission partners to conduct 'deep-dive' conversations on key issues. We also want to include thought leaders outside the Government in these conversations. This discovery process will assist us in developing a target vision and the supporting strategies to build beyond the foundation and accelerate the delivery of the ISE.

To set the stage for the speakers and the dialogue we will be having for the rest of the day – I'd like to briefly describe three ideas.

The first idea. The President's National Security Strategy, released earlier this year, called for a "Whole of Government" approach for strengthening national capacity based on applying and integrating the efforts of all agencies with a national security mission. To effectively support Whole of Government, our working hypothesis is that the ISE must:

- First – Empower the frontline with the information they need to do their job;
- Second - Deliver data-centric shared capabilities that increase reuse;
- Third - Strengthen privacy, civil liberties, and civil rights protections;
- Fourth - Align with technology and information management trends; and

- Finally - Leverage standards-based innovation.

To make the ISE work, we need to focus on data – sharing it, discovering it, protecting it, fusing it, and reusing it. We need a data-centric approach in alignment with the original mandate for the ISE.

I also highlighted standards-based innovation. We can dramatically improve price/performance, increase agility, decrease risk, and accelerate deployment of the ISE by effectively working with our partners in industry.

The second idea. The opening panel is focused on "opening the aperture" to the totality of terrorism-related information as directed in the law. There are several aspects of the "Expanding Aperture" idea:

- In the past, we advanced initiatives in the Federal to State and Local information sharing space. The 2007 National Strategy for Information Sharing does an excellent job laying out roles and responsibilities in this regard.
- Building from our foundation, we want to enhance and extend partnerships with mission partners across all 5 communities – defense, intelligence, homeland security, law enforcement, and foreign affairs. I am looking forward to hearing from today's speakers, as well as members of the audience, on this topic.
- Also, ISE mission partners rarely have the ability to segregate their activities to isolate terrorism-related information. Mission partners ask us for complete solutions. Such needs must be factored into our strategy and plans.

Finally, the third idea is the role of sourcing, integrating, and sharing best practices on the road to transformation. For example – our core standards framework, the National Information Exchange Model is being used well beyond the national security community. Another example is the potential to scale ICD-501-type discovery and dissemination approaches more broadly across the ISE.

We are looking for feedback and discussion – Are these the right ideas? What refinements are necessary? And what is the best way to clarify the target vision and enable incremental progress?

<u>Questions</u>

This brings us into the last parts of my remarks today. We are in the home stretch. We need your help to better understand the landscape, so that the ISE assists our mission partners in delivering comprehensive and inclusive solutions to the issues they face daily. In addition to reacting to the ideas I just highlighted, here are a few questions for the speakers and the participants in today's conference to consider.

a. What are the best practices that should be replicated across Mission Partners?
b. What's the best way to enable discovery?
c. How should we balance data aggregation with decentralized, NSI-type architectures? Is it possible for there to be a single architecture or is the target architecture heterogeneous?

d. The core issue in my opinion with Authorized Use is not technology; it is variability in policies, and lack of consistent, precise semantics for describing those policies. How do we get past these issues?
e. Are there successful examples of imbedding legal restrictions and policies at scale and across domains into automated rules?
f. How should we leverage open government-type ideas to accelerate planning and delivery of the ISE?
g. How do we incentive and celebrate progress in spreading broad adoption of best practices? Is there a role for challenges?
h. And finally, what are the concrete, incremental steps that can be taken to accelerate change this year?

Conclusion

Thank you for listening to my remarks. Hopefully I kept my inner geek in check. I've set the scene to allow us to talk about the future – what the ISE needs to be to support the counterterrorism mission, and how do we accelerate its delivery. I welcome your questions, remarks, and commentary.

###